



Google scholar

date control word key access right EMM OR ma

Search

Advanced Scholar Search

 Search only in Engineering, Computer Science, and Mathematics.

 Search in all subject areas

Scholar

Articles excluding patents ▼

1970

- 2002

include citations ▼



Create email alert Results 1 - 20 of about 15,100. (0.42 sec)

Cryptography for digital TV broadcasting[cuny.edu](#) [PDF]BM Macq, JJ Quisquater - Proceedings of the IEEE, 1995 - [ieeexplore.ieee.org](#)

... **control** wording use as well as a description of the program (identifier, **date**, time, level ... compared to the local entitlements and, if an agreement is found, the **control word** is deciphered ... Once again, the cryptologic habit would use the word "**key**" here rather than "**control word**." We ...

Cited by 314 - [Related articles](#) - [BL Direct](#) - [All 4 versions](#)A calculus for access control in distributed systems[psu.edu](#) [PDF]M Abadi, M Burrows, B Lampson, G ... - ACM Transactions on ..., 1993 - [portal.acm.org](#)

... General Terms: Security, Theory Additional **Key Words** and Phrases: Cryptography, cryptographic protocols, modal logic ... publication and its **date** appear, and notice is given that copying is by permission ... The basic questions of authentication and **access control** are, always, "who ...

Cited by 620 - [Related articles](#) - [BL Direct](#) - [All 72 versions](#)Distributed access-rights management with delegation certificates[rutgers.edu](#) [PDF]

T Aura - Secure Internet Programming, 1999 - Springer

... Sec. 2.3 explains why certificates are an appealing alternative for other methods of distributed **access control**. 2.1 Basic Delegation Certificates subject- ... In the following, we will discuss these and other properties of delegation in detail. Our view of the **world** is **key-oriented**. ...

Cited by 95 - [Related articles](#) - [BL Direct](#) - [All 16 versions](#)Separating key management from file system security[psu.edu](#) [PDF]D Mazieres, M Kaminsky, MF Kaashoek, E ... - ACM SIGOPS ..., 1999 - [portal.acm.org](#)

... Users therefore have a maximal amount of configuration **control** over the file system, which helps eliminate the ... a public **key**, K, and must be signed by the correspond- ing private **key**, K<sup>-1</sup> ... a reliable means of distributing revocation certi- ficates, but it may help get the **word** out fast ...

Cited by 324 - [Related articles](#) - [BL Direct](#) - [All 57 versions](#)Role-based access control on the web[psu.edu](#) [PDF]JS Park, R Sandhu, GJ Ahn - ACM Transactions on Information and ..., 2001 - [portal.acm.org](#)

... However, since this mode is host-based, it cannot support high user mobility, while it may support a more convenient service than the user- based mode, which requires the user's cooperation

(eg, typing in pass- **words**): ... **Date** FALSE 12/31/2001 ... Role-Based **Access Control** • 45 ...

[Cited by 212](#) - [Related articles](#) - [All 21 versions](#)

### Cryptographic solution to a problem of **access control** in a hierarchy

[unisa.it \(PDF\)](#)

SG Akl, PD Taylor - ACM Transactions on Computer Systems ( ...), 1983 - portal.acm.org

... **General Terms**: Security Additional **Key Words** and Phrases: Multilevel security, cryptography, **key**, symmetric and ... It is not difficult to conceive of examples of hierarchies where such **access control** is required ..., of information to be broadcast may, for instance, be the **date** of release ...

[Cited by 335](#) - [Related articles](#) - [All 2 versions](#)

### Cryptographic **key** assignment scheme for dynamic **access control** in a user hierarchy

[ntu.edu.tw \(PDF\)](#)

FH Kuo, VRL Shen, TS Chen, F ... - IEEE Proc-Computers & ..., 1999 - ieeeexplore.ieee.org

... adding some information into the original plaintext M, such as sender identity code, receiver identity code, **date**, and time. ... For an arbitrary poset user hierarchy, we have presented a dynamic **access control** scheme. ... In other **words**, our scheme has been shown to be secure. ...

[Cited by 34](#) - [Related articles](#) - [BI Direct](#) - [All 7 versions](#)

### Smart cards and conditional **access**

[nctu.edu.tw \(PDF\)](#)

L Guillou - Advances in Cryptology, 1985 - Springer

... The card tests its availability and its purchasing power before recording a new operation (**date** and amount). ... A distribution **key** enciphers individual customer **messages** and/or authorization **keys**. ... the **control word** can be sent back on the line to prove user's **right to access**. or ...

[Cited by 10](#) - [Related articles](#) - [All 5 versions](#)

### Cryptographic authentication protocols for smart cards

LC Guillou, M Ugon, JJ Quisquater - Computer Networks, 2001 - Elsevier

... Sold by RSA Security, SecurID cards are more convenient; at each minute, each card provides six decimal digits representing a pseudo-random **date** and time ... the computation of a pair of **control words** (the current ... the crypto-writing of a new **key**, typically a new operation **key**; ...

[Cited by 14](#) - [Related articles](#) - [All 6 versions](#)

### **Key management** and **access control** for large dynamic multicast group

J Liu, M Zhou - 2002 - computer.org

... But to **date**, efficient solutions, especially about the group **key management**, are very few. ... **Key words**: **key management**, **access control**, multicast security ... In our scheme, the **access control** is simplified in some instances (as shown in figure 2). At the same time, the updating ...

[Cited by 8](#) - [Related articles](#) - [All 4 versions](#)

### A binary single-**key**-lock system for **access control**

CK Chang, TM Jiang - IEEE Transactions on Computers, 1989 - ieeeexplore.ieee.org

... In other **words**, we have  $h_0 = K$ ,  $*K$ ,  $Isism$ ,  $Isism$ . ... Then we can conclude that all the row vectors are linearly independent. REFERENCES CJ **Date**, An Introduction of Database Systems, Vol.

9/18/2010

date control word key access right EMM OR manage...

ZZ ... [13] M. Wu and T. Hwang, "Access control with single-key-lock," IEEE Trans. ...

[Cited by 15 - Related articles](#) - [All 6 versions](#)

### Privacy interfaces for information management

[psu.edu](#) [PDF]

T Lau, O Elzioni, DS Weld - Communications of the ACM, 1999 - portal.acm.org

... visited, or to periodically search for all .com pages and mark them private at a later date. ...

Checkboxes **control** whether a setting is applied to the current file, or to all files recursively in ... There

is no way to express a policy such as "Share all Microsoft Word documents, regardless of ...

[Cited by 84 - Related articles](#) - [BI Direct](#) - [All 11 versions](#)

### Towards an access control system for mobile peer-to-peer collaborative environments

[psu.edu](#) [PDF]

P Fenkam, S Dustdar, E Kirda, G Reif, H Gail - 2002 - computer.org

... <AuthorizationCertificate Signature='R24fd64he64hg7448'> <ExpirationDate Date=21.03.2002

Time='15:34'> <Owner ID='fsigmund/'> <Target Type='Telephone' ID='+43699111/'> ... Access control

for collaborative environments. ... [12] World Wide Web Consortium. ...

[Cited by 35 - Related articles](#) - [All 17 versions](#)

### Smart Card a Highly Reliable and Portable Security Device

L Guilou, M Ugon - Advances in Cryptology—CRYPTO'86, 1987 - Springer

... Before reconstructing a **control word**, the card verifies that the current **date** lies in the subscription

period. ... In the card, a 61-bit result (for example, a **control word**) is computed from a 23-bit incoming

parameter, a 127-bit incoming cryptogram, and a 127-bit internal secret **key**. ...

[Cited by 13 - Related articles](#) - [All 2 versions](#)

### Open problems in data-sharing peer-to-peer systems

[stanford.edu](#) [PDF]

N Daswani, H Garcia-Molina, B Yang - Database Theory—ICDT 2003, 2002 - Springer

... Some research has taken place to **date** to specifically address DoS attacks in P2P networks. ... about

the true state of Iraq's nuclear weapons program to the **world** without the fear ... property **management**

and digital **rights management** issues can be cast as **access control** problems. ...

[Cited by 217 - Related articles](#) - [BI Direct](#) - [All 30 versions](#)

### Key processing with control vectors

SM Malayas - Journal of Cryptology, 1991 - Springer

... **Key words**. ... To **date**, cryptographers and implementers of cryptographic standards and products

have evolved **key**-distribution schemes concerned mostly with ... **access** to the **key** is granted, other

more traditional and often more convenient methods of **access control** may be used. ...

[Cited by 17 - Related articles](#) - [All 2 versions](#)

### [PDF] Developing secure agent systems using delegation based trust management

[psu.edu](#) [PDF]

L Kagai, T Finin, A Joshi ... - ... of Mobile MultiAgent Systems (SEMAS 02) ..., 2002 - Citeseer

... are valid, then the receiving agent sends the result back encrypted with the senders public **key**. ...

in the system, how re-delegations are handled, how prohibitions affect **access control** and

9/18/2010

date control word key access right EMM OR manage...

delegations ... In other **words**, a supply chain **management** system consists of a network of ...

[Cited by 37](#) - [Related articles](#) - [View as HTML](#) - All 17 versions

## [\[PDF\] A Key Transport Protocol Based on Secret Sharing--An Application to Conditional Access Systems](#)

[psu.edu](#) [PDF]

AM Eskicioglu, T Multimedia - IS&T/SPIE's 13th International Symposium . . , 2001 - Citeseer

... **Key words**: conditional **access**, content protection, **key** transport, multimedia, public-**key** cryptography, secret ... **Control Messages** (ECMs) carry the descrambling keys (usually called the "**control word**"s in the ... and a brief description of the program (program number, **date**, time, cost ...

[Cited by 3](#) - [Related articles](#) - [View as HTML](#) - All 11 versions

## [Early experience with message-passing on the SHRIMP multicomputer](#)

[psu.edu](#) [PDF]

EW Felten, RD Alpert, A Bilas, MA Blumrich, ... - ACM SIGARCH . . . , 1996 - portal.acm.org

... A **key** question regarding this approach is whether a system built this way ... or distributed for pro d or commercial advantage, the copyright notice, the title of the publication and its **date** appear, and notice is given that copying is by permission of ... strategies, and transfer of **control**. ...

[Cited by 92](#) - [Related articles](#) - [BI Direct](#) - All 26 versions

## [\[citation\] Eurocrypt, a technical approach](#)

JP Clement, F Coutrot, P Fevrier - ... Convention, 1990. IBC . . . , 1990 - ieeexplore.ieee.org

... the **management** centre -the user's viewing time is checked at a later **date** to ensure ... the conditional **access** system depends on the distribution of the service operating **key** and entitlements. ... Security is ensured by the device and frequent replacement of the **control word** for which ...

[Cited by 2](#) - [Related articles](#)

☒ [Create email alert](#)

Googoooooooooooooogle ►

Result Page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)

date control word key access right EMM OR manage... Search

[Go to Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2010 Google

Google scholar

control word key encrypted EMM OR management

Search

[Advanced Scholar Search](#)☒ Search only in Engineering, Computer Science, and Mathematics☐ Search in all subject areas

Scholar

Articles excluding patents ▼

1970

- 2002

include citations ▼



Create email alert Results 1 - 20 of about 7,620. (0.32 sec)

### Cryptography for digital TV broadcasting

[cuny.edu](#) [PDF]BM Macq, JJ Quisquater - Proceedings of the IEEE, 1995 - [ieeexplore.ieee.org](#)

... A second way of **encryption** could be obtained by per- mutations of Huffman **words**, letting low-frequency co- efficiencies be unchanged for transparency. ... Once again, the cryptologic habit would use the **word "key"** here rather than "**control word**." We stick with the terminology ...

[Cited by 314](#) - [Related articles](#) - [BL Direct](#) - [All 4 versions](#)

### Your 80211 wireless network has no clothes

[psu.edu](#) [PDF]WA Arbaugh, N Shankar, YCJ Wan, ... - IEEE Wireless ..., 2002 - [ieeexplore.ieee.org](#)

... as a valid address by programming the desired address into the wireless card, bypassing the access **control** and gaining ... In other **words**, there is no timed **key management** protocol ... which when set along with the authentication option can be used to transport the WEP **key** that is ...

[Cited by 459](#) - [Related articles](#) - [BL Direct](#) - [All 133 versions](#)

### Separating key management from file system security

[psu.edu](#) [PDF]D Mazieres, M Kaminsky, MF Kaashoek, E ... - ACM SIGOPS ..., 1999 - [portal.acm.org](#)

... Users therefore have a maximal amount of configuration **control** over the file system, which helps eliminate the ... Very few servers actually need access to a user's **encrypted** private **key** or SRP data, however ... A server can safely export a public database to the **world** on an SFS file ...

[Cited by 324](#) - [Related articles](#) - [BL Direct](#) - [All 57 versions](#)

### [CITATION] A system for the specification and analysis of key management protocols

C Meadows - ... on Research in Security and Privacy, ..., 1991 - IEEE Computer Society Press

[Cited by 60](#) - [Related articles](#) - [All 2 versions](#)

### [PDF] Applying formal methods to the analysis of a key management protocol

[psu.edu](#) [PDF]

C Meadows - Journal of Computer Security, 1992 - Citeseer

... We identify each processor not under **control** of the penetrator by  $q(ID, honest)$ . ... be divided across two or more rules: one which generates the **word**, and one ... a step in which the originator of an **encrypted message** concatenates **encrypted message**, **encrypted key**, and **message** ...

[Cited by 191](#) - [Related articles](#) - [View as HTML](#) - [All 20 versions](#)

Using encryption for authentication in large networks of computers[psu.edu](#) [PDF]

RM Needham, MD Schroeder - Communications of the ACM, 1978 - portal.acm.org

... **Key Words and Phrases:** **encryption**, security, authentication, networks, protocols, **public-key** cryptosystems, data **encryption** standard ... B's activity if a **message** may only arrive in his security **control** when he ... **Message** 3.2 is **encrypted** with AS's **key** and therefore is accessible only ...

Cited by 2224 - [Related articles](#) - [All 73 versions](#)Dynamic key management schemes for access control in a hierarchy[thu.edu.tw](#) [PDF]

CH Lin - Computer communications, 1997 - Elsevier

... ing kj and r. On the basis of the cryptographic function with elegant properties, the hierarchical **control** protocol is ... his own class, a user in a lower privileged class want to derive the group **key** of his ... In other **words**, owning the values of r, and k, a member in class S, tries to reveal ...

Cited by 83 - [Related articles](#) - [All 8 versions](#)[PDF] Kerberos: An authentication service for open network systems[psu.edu](#) [PDF]

JG Steiner, C Neuman, JI Schiller - Proc. Winter USENIX Conference, 1988 - Citeseer

... Users have com- plete **control** of their workstations: they can reboot them, bring them up standalone ... The authenticator is **encrypted** in the session **key** that is part of the ticket (see Figure 4 ... with the authentication server is designed to minimize the chance that the pass- word will be ...

Cited by 1172 - [Related articles](#) - [View as HTML](#) - [All 297 versions](#)Identity-based information security management system for personal computer networks

E OKAMOTO, K TANAKA - IEEE Journal on Selected Areas in ..., 1989 - ieeexplore.ieee.org

... In this system, we assume a common master **key** MK, and a program to **control** it is stored in all the IC cards. ... work **key** and have IC card decrypt it decrypt the Fig. ... or 24 bit fixed point ALU 55 bit Instruction ROM Data ROM RAM 2 x 512 **word** x 32 bit 2 K **word** x 32 bit 1 K **word** x 32 ...

Cited by 45 - [Related articles](#) - [All 5 versions](#)A calculus for access control in distributed systems[psu.edu](#) [PDF]

M Abadi, M Burrows, B Lampson, G ... - ACM Transactions on ..., 1993 - portal.acm.org

... General Terms: Security, Theory Additional **Key Words and Phrases:** Cryptography, cryptographic protocols, modal logic ... **control**. The basic questions of authentication and access **control** are, always, "who ... the **key** K says s when s is asserted in a **message** decrypted with K. ...

Cited by 620 - [Related articles](#) - [BL Direct](#) - [All 72 versions](#)Using narrowing in the analysis of key management protocols

C Meadows - 1989 - computer.org

... Consider such a protocol from the point of view of a penetrator who has obtained complete **control** of the ... Thus, unless type-checkg is explicitly required in a protocol, a **word** can be used interchangeably as a **message** or as a **key** for **encrypting** a **message**. \* The penetrator has ...

Cited by 60 - [Related articles](#) - [All 7 versions](#)

[\[citation\] A system for the specification and verification of key management protocols](#)

C Meadows - 1991 - computer.org

... term-rewriting model of Dolev and Yso [9]. In their model, the intruder or intruders are assumed to have complete **control** of the ... intruder sees a **word**  $e(k(A), \text{seskey}(N))$ , we assume that he is able to learn that the **word** is indeed  $\text{seskey}(N)$  **encrypted** by A's **key**, even though ...

Cited by 28 - Related articles - All 3 versions

[MARKS: Zero side effect multicast key management using arbitrarily revealed key sequences](#)[psu.edu](#) [PDF]

B Briscoe - Networked Group Communication, 1999 - Springer

... 4. Whenever the time-keeper signals a new game-minute (over the **control** mul- ticast), all the zone ... In other **words**, no branch of the tree ever requires the hash to be calculated more than once ... Receivers can know which **key** to use even if each sender is out of sequence with the ...

Cited by 133 - Related articles - BL Direct - All 16 versions

[A cryptographic key management scheme for implementing the Data Encryption Standard](#)

WF Ehrsam, SM Matyas, CH Meyer, WL ... - IBM Systems ..., 1978 - portal.acm.org

... Cryptographic research conducted dur- ing World War II showed that strong **encryption** systems could be ... into the participating nodes to the extent that the system can **control** the setting of the ... For this reason, the **key management** scheme can be used to protect data stored and ...

Cited by 62 - Related articles - All 4 versions

[Cryptographic solution to a problem of access control in a hierarchy](#)[unisa.it](#) [PDF]

SG Akl, PD Taylor - ACM Transactions on Computer Systems { ..., 1983 - portal.acm.org

... General Terms: Security Additional **Key Words** and Phrases: Multilevel security, cryptography, **key**, symmetric and asymmet- ric ... Cryptographic Solution to a Problem of Access **Control** in a Hierarchy ... at some level of the hierarchy to derive from his own cryptographic **key** the keys ...

Cited by 335 - Related articles - All 2 versions

[Authentication of signatures using public key encryption](#)

KS Booth - Communications of the ACM, 1981 - portal.acm.org

... 4. Merkle, RC Protocols for public **key** cryptosystems. ... analysis (see [2]). Metamodels have also been rec- ommended for mathematical pro- gramming and for world dynamics ... in [3]; they include simulations of job shops, steel plants, medical services, harbors, inventory **control**, etc ...

Cited by 28 - Related articles - All 2 versions

[The RC5 encryption algorithm](#)[psu.edu](#) [PDF]

R Rivest - Fast Software Encryption, 1995 - Springer

... The parameters  $w$ ,  $r$ , and  $b$  in a received or transmitted RC5 **control** block are then merely used for type ... `char key[b]; if (sizeof(WORD)!=4) printf("RC5 error: WORD has %d bytes.\n", sizeof(WORD)); printf("RC5-32 ... on previous ct */ pt[0]=ct[0]; pt[1]=ct[1]; for (j=0;j<b;j++) key[j] = ct[0] ...`

Cited by 693 - Related articles - BL Direct - All 171 versions

[PDF] Why Johnny can't encrypt: A usability evaluation of PGP 5.0[psu.edu \[PDF\]](#)

A Whitten, JD Tygar - Proceedings of the 8th USENIX Security ..., 1999 - Citeseer

... may work for securing a communications channel, but not for setting access **control** policy when a ... the value we expect them to place on their own secrets in the real **world**. ... PGP 5.0 separates these functions into two applications: PGPKeys for **key management**, and PGPTools for ...

[Cited by 524](#) - [Related articles](#) - [View as HTML](#) - [All 67 versions](#)

Formalizing GDOI group **key management** requirements in NPATRL[psu.edu \[PDF\]](#)

C Meadows, P Syverson - Proceedings of the 8th ACM conference ..., 2001 - portal.acm.org

... This allows access **control** for both entering and leaving members to be enforced in an efficient ... In other **words**, the action of stealing a **key** needs to be precipitated by the GCKS ... We have two event statements, one describing the loss of a **key-encryption key**, and one describing ...

[Cited by 28](#) - [Related articles](#) - [All 28 versions](#)

Conditional access system interoperability through software downloading[philips.com \[PDF\]](#)

F Kamperman, B van Rijnsoever - IEEE Transactions on ..., 2001 - ieeexplore.ieee.org

... For security reasons the CW typically changes every few seconds. To protect the **control word** against eavesdropping it is **encrypted** with some cryptographic **key** using a CA-system specific algorithm. ... To **control** access to content, use of the **key** is authorized by entitlement ...

[Cited by 29](#) - [Related articles](#) - [BL Direct](#) - [All 7 versions](#)

[Create email alert](#)

Goooooooooooooogle ►

Result Page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [Next](#)control word key encrypted EMM OR [Go to Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2010 Google



Google scholar

conditional access control word access right en

Search

[Advanced Scholar Search](#)☒ Search only in Engineering, Computer Science, and Mathematics☐ Search in all subject areas

Scholar

Articles excluding patents ▼

1970

- 2002

include citations ▼



Create email alert Results 1 - 20 of about 32. (0.17 sec)

On key distribution management for **conditional access** system on Pay-TV system[ncku.edu.tw](#) [PDF]FK Tu, CS Lai, HH Tung - Consumer Electronics, IEEE ..., 2002 - [ieeexplore.ieee.org](#)...  $cw, l_j = 1, 2, \dots, T+1$ , where  $cw$ , is the time variant **control word** of channel  $j$  ... And subscribers canproduce the **descrambling control** signals in conjunction with keys associated with the ... Tu, Lai and Tung: On Key Distribution Management for **Conditional Access** System on Pay-TV ...[Cited by 62](#) - [Related articles](#) - [BL Direct](#) - [All 4 versions](#)Cryptology for digital TV broadcasting[cony.edu](#) [PDF]BM Macq, JJ Quisquater - Proceedings of the IEEE, 2002 - [ieeexplore.ieee.org](#)... discussion, give a more precise statement of some specific requirements of a **conditional access** system: ... These parameters are read by the **access control** system (decoder), compared to the local entitlements and, if an agreement is found, the **control word** is deciphered ...[Cited by 313](#) - [Related articles](#) - [BL Direct](#) - [All 3 versions](#)**Conditional access** mechanisms for all-digital broadcast signalsD Argebaud, JL Giachetti - Consumer Electronics, IEEE ..., 2002 - [ieeexplore.ieee.org](#)... The **rights** and associated keys needed to **descramble** a programme are called entitlements. ... checks their origin and their integrity before **decrypting** the **control word** and sending it ... 4TECHNIQUES TO APPLY **CONDITIONAL ACCESS** TO DIGITAL BROADCAST PROGRAMMES ...[Cited by 10](#) - [Related articles](#) - [BL Direct](#) - [All 4 versions](#)An overview of security in Eurocrypt **conditional access** systemE Crusellies, JL Melus, M Soriano - ..., 1993, including a ..., 2002 - [ieeexplore.ieee.org](#)... generators and their structure can be seen in figure 5. Before loading them, the **control word** are combined ... service keys will allow it to get the **control words** to **decrypt** the programme. III. ... As can be seen in section 11, the nucleus of the **conditional access** system is the Jeirings ...[Cited by 15](#) - [Related articles](#) - [BL Direct](#)[PDF] Attacks on Pay-TV **access control** systems[freeweb.hu](#) [PDF]MG Kuhn - Security Seminar, Computer Laboratory, Cambridge, 1997 - [freeweb.hu](#)... correction error **conditional access** module ... **Access control** issues: Standardization of Common Scrambling Algorithm will at least allow SimulCrypt, where different **access control** systems can **decrypt** the same **control words** in order to **descramble** the same programme ...

[Cited by 8](#) - [Related articles](#) - [View as HTML](#) - [All 6 versions](#)

### Practical key distribution schemes for channel protection

[nctu.edu.tw](http://nctu.edu.tw) [PDF]

YL Huang, SPW Shieh, JC Wang - Computer Software and ..., 2002 - [ieeexplore.ieee.org](#)

... system can charge his subscribers according to their subscriptions and the intelligent property rights of TV ... These schemes are also a four-level key hierarchy: **Control Word (CW)**, Authorization Key (AK ... SK, the secret key held by the subscriber, is used to **encrypt/ decrypt** the DK. ...

[Cited by 7](#) - [Related articles](#) - [BL Direct](#) - [All 8 versions](#)

### [PDF] A Key Transport Protocol Based on Secret Sharing—An Application to Conditional Access Systems

[psu.edu](http://psu.edu) [PDF]

AM Eskicioglu - IS&T/SPIE's 13th International Symposium on ..., 2001 - Citeseer

... **Control Word** generator ... copy protection are two critical issues that need to be addressed in parallel for the management of **rights** associated with ... The proposed scheme can be a convenient key transport mechanism for **conditional access** systems delivering multimedia content. ...

[Cited by 4](#) - [Related articles](#) - [View as HTML](#) - [All 9 versions](#)

### [PDF] An investigation of the possibility of defining a new conditional access application programming interface for digital television receivers

[psu.edu](http://psu.edu) [PDF]

J Anstensen, HR Nevalainen - Relation, 2002 - Citeseer

... This allows CA systems to filter out their specific **control** data and **descramble** the same service. [DVB ... Page 28. **Conditional access** \_\_\_\_\_ ... Interface modules.

A receiver with CI permits the user to **access** ...

[Cited by 1](#) - [Related articles](#) - [View as HTML](#) - [All 6 versions](#)

### [PDF] Analysis of the nagravision video scrambling method

[psu.edu](http://psu.edu) [PDF]

MG Kuhn - Online document, available at <http://www.ci.cam.ac> ..., 1998 - Citeseer

... we send to the decoder a test image that contains genuine encrypted **control word** information in ... test pixel coordinates (xi,yi) and we branch to the left or the **right** subtree depending ... Since the Nagravision system is anyway scheduled to be replaced by a DVB **conditional access** ...

[Cited by 12](#) - [Related articles](#) - [View as HTML](#) - [All 10 versions](#)

### How to integrate access control mechanisms into digital HDTV systems?

V Michon, JL Giachetti - Signal Processing: Image Communication, 1992 - Elsevier

... draft specification of the digital coding of component TV signals in the range 34-45 Mbits/s [2] ; -

The definition of a new digital Television terrestrial broadcasting; - The **conditional access** on

RDS ... **Free access** means that scrambling uses a fixed **control word** (known by ...

[Related articles](#) - [All 2 versions](#)

### Standardization of conditional access systems for digital pay television

D Van Schooneveld - Philips Journal of Research, 1996 - Elsevier

... necessary includes a generator and an injector for the ECMs and several **control** systems. ... standard developed in a joint effort by many companies throughout the **world** in a ... 112 1996 Standardization

of **conditional access** systems for digital pay television place under fair and ...

[Cited by 5](#) - [Related articles](#) - [BL Direct](#) - [All 2 versions](#)

### [PDF\] Secure delivery of images over open networks](#)

[psu.edu](#) [PDF]

D Augot, JM Boucqueau, JF Delaigle, C ... - Proceedings of the ..., 1999 - CiteSeer

... A **conditional access** system (CAS)[2] aims at managing **access control** for a specified set of users ...

As compared to a World Wide Web search machine, which gives relevant and less relevant information (eg AltaVista gives 40689 responses to "Vinci ... 4.2.1. **Access control** and Logs ...

[Cited by 29](#) - [Related articles](#) - [View as HTML](#) - [BL Direct](#) - [All 15 versions](#)

### [Viper: A multiprocessor SOC for advanced set-top box and digital TV systems](#)

[psu.edu](#) [PDF]

S Dutta, R Jensen, A Rieckmann - Design & Test of ..., 2002 - [ieeexplore.ieee.org](#)

... Enhanced IEEE 1394 link layer Viper includes an IEEE 1394 link layer controller that provides a physical-link-layer interface to the external world. ... The application software handles service accessibility (**conditional access**) and general **control functions**. ...

[Cited by 145](#) - [Related articles](#) - [BL Direct](#) - [All 15 versions](#)

### [PDF\] CERIAS Tech Report 2002-44 A KEY TRANSPORT PROTOCOL BASED ON SECRET SHARING APPLICATIONS TO INFORMATION SECURITY](#)

[psu.edu](#) [PDF]

AM Eskicioglu, EJ Delp - IEEE Transactions on Consumer Electronics, 2002 - CiteSeer

... A **conditional access** (CA) system [31, (41 is a system that allows **access** to services ... The service and the entitlement messages indicating the **access** conditions are protected at the CA ... **Control** Messages (ECMs) carry the **descrambling** keys (usually called the "control word"s in ...

[View as HTML](#) - [All 3 versions](#)

### [Digital Watermarking based Key Distribution Method for Pay-TV System](#)

[nsysu.edu.tw](#) [PDF]

YH Ke - 2000 - [etd.lib.nsysu.edu.tw](#)

... 23 1.9 DEFINING KEYS .....23 1.9.1 **Control Word** (CW) .... 23 ... This function is called **Conditional Access** System (CAS) [1]. Because the programs in pay-channels ... the order left to **right**, and top to down. ...

[Related articles](#) - [All 3 versions](#)

### [An overview of multimedia content protection in consumer electronics devices](#)

[psu.edu](#) [PDF]

AM Eskicioglu, EJ Delp - Signal Processing: Image Communication, 2001 - Elsevier

... Such architectures are considered extensions of **conditional access** systems, restricting viewing when the consumer does ... The DVD Copy **Control** Association (CCA) is the entity created to license the ... The CSS Specifications are provided for each licensee to have **access** to the ...

[Cited by 122](#) - [Related articles](#) - [All 26 versions](#)

### [HTML\] Chip Architecture](#)

[computer.org](#) [HTML]

S Dutta, P Semiconductors, R Jensen, A ... - IEEE DESIGN & TEST ..., 2001 - [computer.org](#)

... Enhanced IEEE 1394 link layer. Viper includes an IEEE 1394 link layer controller that provides a physical-link-layer interface to the external world. ... The application software handles service

accessibility (**conditional access**) and general **control** functions. ...

[Related articles](#) - [Cached](#) - [All 2 versions](#)

### The DMAC packet transmission system for UK DBS

PL Segar - UK Direct Broadcast Satellite, IEE Colloquium on, 2002 - [ieeexplore.ieee.org](#)

... SI and **conditional access** data have had their share ... The potential of this for a multitude of data-cast services offering financial, or stock **control** information for example is considerable, and will almost certainly lead to data-only receivers being produced that may resemble more ...

[Related articles](#)

### [PDF] A UNIFIED PCA AND DSP BASED POD MODULE FOR HYBRID CRYPTOSYSTEMS

N Zhang - 2000 - [collectionscanada.gc.ca](#)

[collectionscanada.gc.ca](#) [PDF]

... According to the content **control** information, a decision is made if the message needs to be ... The POD reencrypts the content which has **decrypted** under the **conditional access** system and culpuled ... content which is delivered with free **rights** to copy, and free **access** broad- cast ...

[Related articles](#) - [All 3 versions](#)

### Broadband network delivery of interactive digital video using ATM

W Mao - The Journal of VLSI Signal Processing, 1997 - Springer

... In other **word**, the com- plete ATM cells in the frame will be passed into the higher layers for further processing. ... Additional session management of VDT **access** network (from headend to home) can use DSM- CC (Digital Storage Media—Command and **Control**) of MPEG as ...

[Cited by 1](#) - [Related articles](#) - [BL Direct](#) - [All 4 versions](#)



[Create email alert](#)

Google ►

Result Page: 1 2 [Next](#)

conditional access control word acces

[Go to Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2010 Google